

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:  
**Bernhard Förstl**

Serial No.:

Filing Date: **April 9, 2004**

Title: **Method and Device for Increasing the  
Safety of Operation of an Electrical  
Component**

§  
§  
§  
§  
§  
§  
§  
§  
§  
§

Group Art Unit:

Examiner:

Attny. Docket No. **071308.0546**

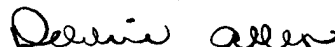
Client Ref.: **2002P20781US**

Mail Stop Patent Application  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

CERTIFICATE OF MAILING VIA EXPRESS MAIL

PURSUANT TO 37 C.F.R. § 1.10, I HEREBY CERTIFY THAT I HAVE INFORMATION AND A REASONABLE BASIS FOR BELIEF THAT THIS CORRESPONDENCE WILL BE DEPOSITED WITH THE U.S. POSTAL SERVICE AS EXPRESS MAIL POST OFFICE TO ADDRESSEE, ON THE DATE BELOW, AND IS ADDRESSED TO:

MAIL STOP PATENT APPLICATION  
COMMISSIONER FOR PATENTS  
P.O. Box 1450  
ALEXANDRIA, VA 22313-1450



EXPRESS MAIL LABEL: EV339228534US  
DATE OF MAILING: APRIL 9, 2004

SUBMISSION OF PRIORITY DOCUMENT

Dear Sir:

We enclose herewith a certified copy of German patent application DE 103 16 805.2 which is the priority document for the above-referenced patent application.

Respectfully submitted,  
BAKER BOTTS L.L.P. (023640)

Date: April 9, 2004

By:



Bruce W. Slayden II  
One Shell Plaza  
910 Louisiana Street  
Houston, Texas 77002-4995  
Telephone: 713.229.1786  
Facsimile: 713.229.7886  
ATTORNEYS FOR APPLICANTS



## Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

**Aktenzeichen:** 103 16 805.2

**Anmeldetag:** 11. April 2003

**Anmelder/Inhaber:** Siemens Aktiengesellschaft,  
München/DE

**Bezeichnung:** Verfahren und Vorrichtung zur Erhöhung  
der Betriebssicherheit einer elektrischen  
Komponente

**IPC:** G 05 B, H 02 P, G 06 F

**Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.**

München, den 17. Dezember 2003  
**Deutsches Patent- und Markenamt**  
**Der Präsident**  
Im Auftrag

## Beschreibung

Verfahren und Vorrichtung zur Erhöhung der Betriebssicherheit einer elektrischen Komponente

5

Die vorliegende Erfindung betrifft ein Verfahren zur Erhöhung der Betriebssicherheit einer oder mehrerer elektrischer Komponenten, insbesondere elektrischer Komponenten in einem Fahrzeug, gemäß dem Oberbegriff von Anspruch 1 und eine dementsprechend ausgebildete Vorrichtung nach dem Oberbegriff von Anspruch 6.

10

Unter dem Begriff der elektrischen Komponenten sollen im Rahmen der vorliegenden Erfindung auch elektronische Komponenten verstanden werden. Elektrische Schutzvorrichtungen zur Erhöhung der Betriebssicherheit elektrischer Komponenten sind seit langem bekannt. Allen benannten Bauformen von elektrischen Schutzvorrichtungen ist jedoch gemeinsam, dass sie z.B. als Schmelzsicherungen auch in der Form von Chip- oder Mikrosicherungen zum Schutz von Leistungsversorgungs- und Kontrollfunktionen durch einen jeweils beanspruchten Bauraum zunehmend schwerer in Schaltungen integrierbar sind.

15

20

Eine besonders gravierende Situation tritt innerhalb einer Fahrzeug-Elektronik oder einer Fahrzeug-Controllereinheit auf. Hierauf wird nachfolgend exemplarisch im Detail eingegangen. Im Kraftfahrzeugbereich werden hohe Anforderungen an die Sicherheit von Fahrgästen und Fahrzeugführen gestellt. Der Umfang von elektrisch abzusichernden Leistungsfunktionen wird so insbesondere in Personenkraftfahrzeugen in naher Zukunft insgesamt weiterhin stark anwachsen, und damit auch die Anzahl von Fahrzeug-Controllereinheiten. Ein jeweils vorhandener Platz für derartige Einheiten ist jedoch stark be-

25

30

grenzt. So verursacht eine Integration von elektrischen Schutzmaßnahmen in Controllereinheiten im Hinblick auf eine jeweilige Platzierung und einen jeweiligen Raumbedarf schon heute große Probleme.

5

Jenseits eines einfachen Überlastungsschutzes, also eines Schutzes gegen zu hohe Ströme, Spannungen, Temperaturen etc. sind Schutzvorrichtungen noch wesentlich komplexer. Auch in ihrer Realisation sind derartige Schutzvorrichtungen aufwen-  
10 diger, als z.B. eine Schmelzsicherung. Diese Schutzvorrich-  
tungen werden üblicher Weise als Mikrocontrollerschaltungen ausgeführt, deren Aufgabe auch in der Überwachung der Funkti-  
on angeschlossener oder zu schaltender Lasten liegt. So stel-  
len beispielsweise die Motoren einer Zentralverriegelungsvor-  
15 richtung innerhalb eines Kraftfahrzeugs Lasten dar, die in  
der Applikation als niederohmige Lasten bei vergleichsweise hohen Strömen nur sehr kurzzeitig betätigt werden, in der Re-  
gel nur ca. 400ms lang. Diese kurze Ansteuerungszeit reicht  
aus, um die Zentralverriegelung eines Fahrzeugs in den ge-  
20 wünschten Zustand zu bringen. Aufgrund der kurzen Ansteuer-  
zeit können die Querschnitte der Leitungen, die elektrischen  
Komponenten, deren Auslegung und Dimensionierung bzw. allge-  
mein gesprochen der Aufwand für eine Verlustwärmeableitung  
eines hohen Stromflusses dennoch gering gehalten werden.

25

Bei bekannten und vorveröffentlichten Sicherheitsvorrichtun-  
gen der Anmelderin erfolgt die Diagnose einer jeweils zu  
schaltenden Hochstromlast oder eines sicherheitsrelevanten  
Verbrauchers entweder vor dem Einschalten der Last oder un-  
30 mittelbar nach Aktivierung des entsprechenden Ausgangs an ei-  
nem Controller. Dabei ist der Controller im Wesentlichen auch  
nur während der Zeitspanne aktiv geschaltet, in der die je-  
weilige Last anzusteuern ist. Ein zeitlich zwischen den ge-

nannten Zeitpunkten auftretendes Fehlverhalten kann dadurch prinzipiell nicht detektiert werden. Eine unerkannte Störung kann somit zu sicherheitskritischen Betriebszuständen führen und z.B. einen Kabelbrand im Fahrzeug hervorrufen, oder aber  
5 eine unerwünschte und unkontrollierte Aktivierung sicherheitsrelevanter Stellglieder bewirken.

Aufgabe der vorliegenden Erfindung ist es, eine verbesserte Vorrichtung und ein Verfahren zur Erhöhung der Betriebssicherheit einer oder mehrerer elektrischer Komponenten unter  
10 Berücksichtigung der vorstehend genannten Art von Fehlermechanismen zu schaffen.

Diese Aufgabe wird erfindungsgemäß durch ein Verfahren mit  
15 den Merkmalen von Anspruch 1 sowie durch ein System als Vorrichtung mit den Merkmalen von Anspruch 6 gelöst.

Eine Vorrichtung zur Erhöhung der Betriebssicherheit elektrischer Komponenten als Last weist demnach erfindungsgemäß Detektionsmittel zum aktiven Detektieren einer Schaltzustandsänderung einer jeweiligen Last auf, die unabhängig von einem  
20 Zeitpunkt einer aktiven Ansteuerung eines Mikrocontrollers auf den Mikrocontroller und/oder eine übergeordnete Kontrolleinheit einwirken.

In einer Weiterbildung der Erfindung wird eine Diagnoserückführung auf einen „wake up“-fähigen Interrupt-Eingang gelegt, vorzugsweise einen Interrupt des Mikrocontrollers als Kontrollorgan. In einer Ausführungsform der Erfindung wird zur  
25 Diagnoserückführung ein Eingang für einen nicht ausblendbaren bzw. non maskable Interrupt als Diagnose-Rücklese-Port benutzt. Alternativ werden Rückmeldungen über eine Zustandsänderung über einen Bus an eine übergeordnete Kontroll-Instanz  
30

versandt. Als verbreiteten Bus-Standard bietet sich bei Kraftfahrzeugen der CAN-Bus mit der Möglichkeit einer Priorisierung bestimmter Meldungen an.

- 5 Ferner wird vorteilhafterweise eine Diagnose durchgeführt. Dabei wird festgestellt, ob der vorliegende Fehler durch den Mikrocontroller alleine überhaupt behoben werden kann. Im Fall eines gravierenden Fehlers ohne Korrekturmöglichkeit durch den Mikrocontroller wird eine Abschaltung oder eine an-  
10 dere Maßnahme zur Abhilfe durch eine dem Mikrocontroller übergeordnete Instanz vorgenommen.

Weitere vorteilhafte Ausgestaltungen sind Gegenstand der jeweiligen Unteransprüche.

15

- Die vorliegende Erfindung wird nachfolgend zur Darstellung weiterer Merkmale und Vorteile unter Bezugnahme auf die beigefügte Zeichnung anhand bevorzugter Ausführungsbeispiele in  
20 schematischer Darstellung näher erläutert. Es zeigen:

Figur 1: eine Prinzipskizze eines erfindungsgemäßen Schaltkreises;

- 25 Figur 2: eine Darstellung eines Zeitverhaltens im Störfall;

Figur 3: eine Darstellung eines erweiterten Schaltkreises mit einer nicht aktiv behebbaren Störung;

30

Figur 4: eine Prinzipskizze eines Schaltkreises nach dem Stand der Technik und

Figur 5: eine Darstellung eines Zeitverhaltens des Schaltkreises nach Figur 4 in einem Störfall.

5 Ein Schaltkreis 1 nach dem Stand der Technik umfasst als steuerndes Element einen Mikrocontroller  $\mu C$ , der durch ein Steuersignal  $l_{ctrl}$  eine Last über einen Leistungsverstärker oder Schalter L ansteuert, siehe Figur 4. Die Last, hier ein Motor M, erhält ein Ansteuersignal  $l_{act}$ . Dieses Ansteuersignal  
10  $l_{act}$  wird hier über einen Spannungsteiler als Diagnosesignal Diag teilweise an den Mikrocontroller  $\mu C$  zurückgeführt. Hierdurch wird bestätigt, dass das Steuersignal  $l_{ctrl}$  auch durch das Ansteuersignal  $l_{act}$  zum Einschalten des Motors M korrekt umgesetzt worden ist.

15 Eine solche Schaltung 1 wird bekannter Weise in Kraftfahrzeugen zur Ansteuerung und Kontrolle von Motoren M einer Zentralverriegelungsvorrichtung eingesetzt. Die Motoren M stellen hierbei eine niederohmige Last dar, die mit hohen Strömen nur  
20 kurzzeitig angesteuert werden. Die kurze Ansteuerzeit von z.B. 400ms reicht jedoch aus, um die Zentralverriegelung eines Fahrzeugs in den gewünschten Zustand zu bringen. Aufgrund der kurzen Ansteuerzeit können die Querschnitte der Leitungen und die elektrischen Komponenten in ihrem gesamten Dimensio-  
25 nierung im Hinblick auf eine Ableitung von Verlustwärme gering gehalten werden, obgleich in einem aktiven Zustand der Schaltung relativ hohe Ströme fließen.

Eine Diagnose eines Motors M als zu schaltender „Hochstromlast“ erfolgt durch den Mikrocontroller  $\mu C$  in einem Zeitfenster, das in der Abbildung von Figur 5 strich-punktiert umrandet ist. Die Diagramme von Figur 5 stellen den zeitlichen Signalverlauf in dem Mikrocontroller  $\mu C$  anhand eines hin-

durchfließenden Stromes  $I$  und den Verlauf des Ansteuersignals  $l_{act}$  dar, das an der Last  $M$  anliegt.

Der Signalverlauf in dem Mikrocontroller  $\mu C$  zeigt, dass generell Perioden  $T_{\mu C run}$  mit aktivem Mikrocontroller  $\mu C$  von Zeitabschnitten zu unterscheiden sind, in denen der Mikrocontroller  $\mu C$  in einen Ruhemodus geschaltet ist. Perioden im Ruhemodus sind mit  $T_{\mu C stop}$  gekennzeichnet. Demnach erfolgt eine Diagnose des Motors  $M$  im vorliegenden Fall zu einem Zeitpunkt  $t_1$  vor dem Einschalten der Last  $M$  und zu einem Zeitpunkt  $t_2$  unmittelbar nach Aktivierung des entsprechenden Ausgangs am Controller  $\mu C$ . In beiden Fällen muss der Mikrocontroller  $\mu C$  aktiv geschaltet bzw. eingeschaltet sein. Alternativ kann auch einer dieser Diagnosezustände wenigstens nach dem Stand der Technik als ausreichend erachtet werden. Diese Möglichkeiten werden hier nicht weiter verfolgt.

Durch nicht weiter dargestellte Steuersignale  $l_{ctrl}$  wird nun bei eingeschaltetem Mikrocontroller  $\mu C$  die Last  $M$  selber kontrolliert und geregelt für eine Zeitspanne  $T_a$  aktiv geschaltet. Es schließt sich an diese Aktivphase  $T_a$  von 400ms bei dem Antriebsmotor  $M$  einer Zentralverriegelungseinrichtung eine Ruhephase  $T_i$  mit deaktivierter Last  $M$  an. In der Ruhephase  $T_i$  ist der Mikrocontroller  $\mu C$  selber auch abgeschaltet, wie durch den Abschnitt  $T_{\mu C stop}$  in dem Diagramm von Figur 5 mit dem geringen Stromfluss durch den Mikrocontroller  $\mu C$  gekennzeichnet ist.

Zu einem Zeitpunkt  $t_s$  verursacht nun eine äußere Störung  $S$  ein unerwünschtes Aktivieren der Last  $M$  über einen Zeitraum  $T_{a*}$ . Hier wird diese Störung  $S$  als magnetischer Puls in dem Steuersignal  $l_{ctrl}$  angenommen. Diese vergleichsweise schwache Störung  $S$  wird in der Schaltung nach Figur 4 durch den Leis-



tungsverstärker L verstärkt. Das Störungssignal S ist damit von einem erwünschten Steuersignal  $l_{ctrl}$  nicht zu unterscheiden und aktiviert so die Last M. Dieses auf einer relativ schwachen magnetischen Störung S basierende Fehlverhalten liegt zeitlich nicht zwischen den Zeitpunkten  $t_1$  und  $t_2$  in einem Zeitraum  $T_{\mu C stop}$ , in dem der Mikrocontroller  $\mu C$  als Kontrollorgan selber auch abgeschaltet ist. Damit kann dieses Fehlverhalten nicht detektiert werden.

Das kann zu einem sicherheitskritischen Zustand in dem Fahrzeug führen: Die Last M wird nun dauerhaft mit einem hohen Strom beaufschlagt. Hierdurch geht viel elektrische Energie verloren. Andererseits ist die gesamte Elektrik eines Kraftfahrzeugs hinsichtlich der Abfuhr von Verlustwärme nicht auf eine derartige Dauerbelastung ausgelegt. Nach Überschreiten einer Zeitspanne  $\Delta t_d$  ist daher mit einer dauerhaften Beschädigung einer oder mehrerer elektrischer und elektronischer Einrichtungen zu rechnen. Diese Beschädigung ist durch den Blitz in Figur 5 angedeutet. Aber auch größere Schäden, wie z.B. ein Kabelbrand im Fahrzeug oder eine Aktivierung weiterer sicherheitsrelevanter Stellglieder, sind nicht auszuschließen.

Auch von der Einbruchs- und Diebstahlssicherheit her betrachtet ist dieser Zustand unzufriedenstellend: Ein Kontrollsystem eines sicherheitsrelevanten Verbrauchers, wie hier die Ansteuerung eines Motors M einer Zentralverriegelung, kann mittels eines magnetischen Störimpulses von ca. 400ms Dauer sehr effektiv ausgeschaltet werden. Das Fahrzeug wäre damit durch äußere Manipulation z.B. an mindestens einer Tür geöffnet worden. Zudem könnte eine derartige Manipulation auch zerstörungsfrei vorgenommen werden, so dass sie insbesondere versicherungstechnisch nicht nachweisbar sein könnte.

Bisher wurde die vorstehende Art von Fehlermechanismen nicht betrachtet. Folglich werden derartige Störungen durch bekannte Sicherheitsvorrichtungen auch nicht abgedeckt. Elektrische Sicherheitsanforderungen und ein verbesserter Manipulationsschutz an einem Fahrzeug fordern hier Abhilfe.

Die Diagnose der geschalteten Hochstrom- und/oder sicherheitsrelevanten Lasten M wird nachfolgend durch eine aktive Detektion einer Schaltzustandsänderung einer jeweiligen Last M erweitert. Dabei erfolgt diese Diagnose unabhängig von einem Zeitpunkt einer aktiven Ansteuerung der Last M durch den Mikrocontroller  $\mu C$ . Die Last M kann aber zusätzlich auch weiterhin unmittelbar vor dem Einschalten und/oder unmittelbar nach dem Einschalten diagnostiziert werden, worauf hier aber nicht weiter eingegangen werden soll.

Die Diagnoserückführung wird auf einen sog. „wake up“-fähigen Interrupt-Eingang IRQ des Mikrocontrollers  $\mu C$  gelegt. Dies ermöglicht eine aktive Diagnose bei einer Zustandsänderung der Last M auch in dem Fall, dass der Controller  $\mu C$  sich in einem Stopp-Modus oder Power down mode  $\mu C_{stop}$  während einer Zeitspanne  $T_{\mu C stop}$  befindet.

Neben den wake up-fähigen Interrupt-Eingängen IRQ an dem Controller  $\mu C$  ist ein Ein-/Ausgang I/O für einen sog. non maskable Interrupt, kurz NMI, als Diagnose-Rücklese-Port geeignet. Die Verwendung des NMI-Interrupts ist äußerst wirkungsvoll und vorteilhaft, da diese Interrupt-Routine softwaremäßig nicht maskiert, nicht ausgeblendet oder disabled werden kann. Sie wird damit auch trotz möglicherweise vorhandenen sonstigen Prozessorstörungen in jedem Fall ausgeführt.

Eine erfindungsgemäße Abwandlung der Prinzipskizze eines Schaltkreises 1 nach dem Stand der Technik gemäß Figur 4 ist in Figur 1 wiedergegeben. Es ist dabei darauf hinzuweisen, dass wake up-fähigen Interrupt-Eingänge IRQ und auch Eingänge für non maskable Interrupts NMI an bekannten Mikrocontrollern oder deren Chip-Familien bereits heute ausgeführt und damit bei vertretbaren Mehrkosten verfügbar sind.

Ein Zeitverhalten der Schaltung nach Figur 1 ist in der Abbildung von Figur 2 wiedergegeben. Die Beschreibung dieses Zeitverhaltens wird hier auf einen Störfall beschränkt: Während sich der Mikrocontroller  $\mu C$  in einem Stopp Modus oder Power down mode  $\mu C_{stop}$  befindet wirkt wiederum zu dem Zeitpunkt  $t_s$  die äußere Störung S als magnetischer Impuls oder sonstiger Einstreuung auf die Schaltung 1 ein. Wie zu Figur 5 vorstehend beschrieben wird ohne Vorgabe durch den Mikrocontroller  $\mu C$  die Last M aktiviert. Nur löst diese Änderung des Zustandes der Last M im Gegensatz zu Vorrichtungen nach dem Stand der Technik jetzt einen Interrupt IRQ aus, der sofort an den entsprechenden Eingang des Mikrocontrollers  $\mu C$  weitergeleitet wird. Innerhalb einer sehr kurzen Zeitspanne  $\Delta t_{reg}$  von der Auslösung des Interrupts IRQ bis zu dessen Verarbeitung innerhalb des Mikrocontrollers  $\mu C$  hält ein Zeitabschnitt  $\Delta t_{a*}$  mit aktivem Zustand der Last M ohne Kontrolle durch den Mikrocontroller  $\mu C$  an. Danach ist der Mikrocontroller  $\mu C$  ab dem Zeitpunkt  $t_w$  in den aktiven Zustand  $\mu C_{run}$  geschaltet worden. Eine neue Periode  $T_{\mu C_{run}}$  beginnt, und damit werden von nun an die Zustände aller Lasten M überprüft, die mit diesem Mikrocontroller  $\mu C$  verbunden sind. So können rasch eine oder mehrere insbesondere sicherheitsrelevante Lasten M auf ihren jeweiligen Schaltzustand überprüft werden.

Eine Zeitspanne, die für diese Überprüfung maximal vorgesehen ist, ist als  $\Delta t$  in der Zeichnung von Figur 2 dargestellt.

Die Zeitspanne  $\Delta t$  ist in diesem Beispiel geringer als die Zeitdauer  $T_{\mu C_{run}}$ , während derer der Mikrocontroller  $\mu C$  mit Überwachungsaufgaben in den aktiven Zustand  $\mu C_{run}$  geschaltet bleibt. Innerhalb der Zeitspanne  $\Delta t$  kann der Mikrocontroller  $\mu C$  zu jedem Zeitpunkt die Last  $M$  wieder deaktivieren und damit die Periode  $T_{a*}$  beenden. Jeweils erforderliche Schaltdauern von ca. 400 ms zum Schalten einer Zentralverriegelung mit Sicherheit werden nicht erreicht, da jede Messung für eine sicherheitsrelevante Last  $M$  nur wenige Millisekunden lang andauert. Insbesondere aber ist die Zeitspanne  $\Delta t$  geringer als die zu Figur 5 beschriebene Aufheizperiode  $\Delta t_d$ , nach deren Ablauf mit einer Beschädigung elektrischer Komponenten durch Überhitzung zu rechnen ist.

In einer alternativen Ausführungsform der Erfindung greift eine Regelung über Steuerbefehle nach dem Controller area network-Standard ein, kurz CAN. Auf der Basis beispielsweise einer Zweidrahtleitung werden nach dem CAN-Standard Steuerbefehle, sog. CAN-messages, über ein Datennetz versendet. Gelesen werden diese Steuerbefehle von allen an diesen Bus angeschlossenen Geräten, ausgewertet hingegen nur von einem jeweils adressierten Gerät. Hierbei kann jeweils zusätzlich die Bedeutung einer Nachricht durch Wahl einer Prioritätsstufe hervorgehoben werden. Eine hohe Priorität einer CAN-message, die durch die Störung  $S$  und die damit verbundene Zustandsänderung ausgelöst wurde, garantiert eine sofortige Reaktion des Mikrocontrollers  $\mu C$  nach dessen Einschalten bzw. Erreichen des Zustandes  $\mu C_{run}$ . Mit dem Verstreichen der Verarbeitungszeitspanne  $\Delta t_{reg}$  kann damit der Last  $M$  also sofort unter

Behebung des Fehlerzustandes aus dem Aktivzustand wieder definiert in den deaktivierten Zustand überführt werden.

Es können somit also Fehlerzustände schnell erkannt und sicher behoben werden, die durch äußere elektromagnetische Beeinflussung bzw. in Manipulationsabsicht durch hochenergetische Impulse ausgelöst werden. Neben von außen hervorgerufenen Fehlerzuständen können in einem Fahrzeug jedoch auch Fehlfunktionen auftreten, die durch den Mikrocontroller  $\mu C$  selber nicht mehr aktiv zu beseitigen sind. Als solche Fehlerzustände werden z.B. Fehler in dem Mikrocontroller  $\mu C$  selber betrachtet. Sie können in der Form durchlegierter Gatter oder Ports in dem Mikrocontroller  $\mu C$  auftreten. Bei einem als Mikrocontroller  $\mu C$  verwendeten wiederbeschreibbaren elektronischen Baustein können jedoch aufgrund einer als „moving bits“ bezeichneten Erscheinung auf Dauer zudem Fehler in seiner Programmierung auftreten. Im ersten Fall ist der Mikrocontroller  $\mu C$  selber defekt und kann nur noch ausgetauscht werden, im zweiten Fall ist eine Abhilfe durch erneute Programmierung möglich. In beiden Fällen kann der Mikrocontroller  $\mu C$  jedoch selber die Fehlerzustände nicht mehr beheben.

Auch Fehler in einer Verkabelung oder einem Kabelbaum an der zu schaltenden Last M mit einem Kurzschluss der Last M beispielsweise von einer Versorgungsspannung  $+U_{bat}$  nach Masse GND können erkannt, aber nicht durch den Mikrocontroller  $\mu C$  behoben werden. Hierzu ist in der Abbildung von Figur 3 ein Schaltkreis 1 mit einem Steuergerät SG und einem Bordnetz-Steuergerät BS zur Ansteuerung eines Motors M dargestellt, wobei das Steuergerät dem nicht weiter dargestellten Mikrocontroller  $\mu C$  übergeordnet ist. Der Motor M weist hier einen Kurzschluss nach Masse als plötzlich aufgetretenen Fehlerzustand auf. Durch die von der Zustandsänderung auf der Basis

des Diagnosesignals Diag ausgelösten Diagnose wird dieser gravierende Fehlerzustand an der Last M festgestellt. Es steht somit auch fest, dass dieser Fehler nicht durch den Mikrocontroller  $\mu C$  behoben werden kann. Nach dieser Klassifizierung des Fehlers wird durch das Steuergerät SG eine Fehler-Nachricht über den Daten-Bus ausgegeben und veranlasst das Bordnetzsteuergerät BS als Abhilfemaßnahme die Versorgungsspannung des fehlerhaften Schaltkreises abzuschalten und eine Fehleranzeige zu aktivieren.

Eine zügige und zuverlässige Umsetzung der CAN-message ist innerhalb des dargestellten Ausschnitts des Bordnetzes dadurch sichergestellt, dass nach dem CAN-Standard Nachrichten unterschiedliche Prioritäten eingeräumt werden können. Bei Fehlerzuständen in sicherheitsrelevanten Teilen kann damit eine hohe Priorität voreingestellt werden. Dadurch können gezielt Maßnahmen zum Systemschutz eingeleitet werden, hier nämlich ein Deaktivieren der fehlerhaften Last durch aktive Abschaltung des entsprechenden Schaltkreises, da der Mikrocontroller  $\mu C$  diesen Fehler nicht beheben kann. Im vorliegenden Fall nach Figur 3 lautet der Inhalt der CAN-message mit hoher Priorität somit: „Schalte Stromversorgung des Motors M sofort ab.“ Diese Nachricht wird in jedem Fall ausgeführt und prioritär umgesetzt. Damit werden schnell und effektiv Kabelbrände oder Steuergerätabbrand, aber auch eine Entladung der Batterie vermieden.

Insgesamt ist damit vorstehend ein zuverlässiges Verfahren zur Erhöhung der Betriebssicherheit elektrischer Komponenten realisiert worden, das auf der Basis einer Überwachung unbeabsichtigter Zustandsänderungen von schaltbaren kritischen Lasten aufbaut. Auch bei einem erfindungsgemäßen Verfahren muss der Mikrocontroller oder ein übergeordnetes Steuergerät

nicht permanent in einem aktiv Run-mode betrieben werden. Damit ist eine zusätzliche Sicherheitsfunktion angegeben worden, durch deren Umsetzung der Stromverbrauch der steuernden Elektronikereinheit im Wesentlichen nicht erhöht wird. Die Betriebssicherheit ist jedoch erheblich gesteigert worden, während der apparative Aufwand insgesamt fast gleich geblieben ist. Durch die unterschiedliche Codierung über Interrupts oder über CAN-messages wird eine Umsetzung sicher durchgeführt.

10

Durch eine Erweiterung der Auswerte- und Analysefähigkeiten eines Mikrocontrollers  $\mu C$  und/oder eines übergeordneten Steuergerätes SG können die diskutierten Anwendungsmöglichkeiten auch kumulativ zu bekannten Sicherheitsverfahren zur Steigerung einer Gesamtsicherheit beispielsweise in einem Fahrzeug redundant herangezogen werden. Die Kosten für zusätzliche Hardware sind dabei im Wesentlichen auf einen Mikrocontroller-Baustein beschränkt, der jedoch in Sicherheitsvorrichtungen der vorstehend genannten Art als Bauteil an sich bereits vorgesehen ist. Eine Nachrüstung kann daher auch in Form eines Austausches eines Mikrocontrollers als standardisiertes elektronisches Bauteil vorgenommen werden, in dem nun zusätzlich erforderliche Hardware zusammengefasst ist.

15

20

## Patentansprüche

1. Verfahren zur Erhöhung der Betriebssicherheit einer elektrischen Komponente, insbesondere von elektrischer Komponenten in einem Fahrzeug,  
bei dem eine Last (M) über einen Mikrocontroller ( $\mu$ C) angesteuert wird,  
d a d u r c h g e k e n n z e i c h n e t, dass eine Schaltzustandsänderung einer jeweiligen Last (M) aktiv detektiert wird, wobei eine Diagnose unabhängig von einem Zeitpunkt einer aktiven Ansteuerung der Last (M) durch den Mikrocontroller ( $\mu$ C) und/oder durch eine übergeordnete Kontrolleinheit (SG) erfolgt.
2. Verfahren nach Anspruch 1,  
d a d u r c h g e k e n n z e i c h n e t, dass die Diagnoserückführung auf einen wake up-fähigen Interrupt-Eingang (IRQ) des Mikrocontrollers ( $\mu$ C) gelegt wird.
3. Verfahren nach einem der beiden vorhergehenden Ansprüche,  
d a d u r c h g e k e n n z e i c h n e t, dass die Diagnoserückführung auf einen Eingang (I/O) für einen non maskable Interrupt (NMI) als Diagnose-Rücklese-Port gelegt wird.
4. Verfahren nach einem der vorhergehenden Ansprüche,  
d a d u r c h g e k e n n z e i c h n e t, dass das Ein- oder Abschalten einer Last (M) durch ein Bordnetz-Steuergerät (BS) durchgeführt wird, wobei als Last (M) vorzugsweise ein Motor einer Zentralverriegelung angesteuert wird.
5. Verfahren nach einem der vorhergehenden Ansprüche,  
d a d u r c h g e k e n n z e i c h n e t, dass durch ein Diagnosemittel festgestellt wird, ob eine Fehlerzustand durch den Mikrocontroller ( $\mu$ C) behoben werden kann,



wobei durch eine übergeordnete Kontrolleinheit (SG) bei Versagen des Mikrocontroller ( $\mu$ C) Abhilfemaßnahmen eingeleitet werden.

- 5 6. Vorrichtung zur Erhöhung der Betriebssicherheit einer elektrischen Komponente in einer Schaltung (1), insbesondere von elektrischer Komponenten in einem Fahrzeug, bei der eine Last (M) mit einem Mikrocontroller ( $\mu$ C) zur Ansteuerung verbunden ist,
- 10 d a d u r c h g e k e n n z e i c h n e t, dass die Vorrichtung Mittel zur aktiven Detektion einer Schaltzustandsänderung der Last (M) aufweist, die unabhängig vom Zeitpunkt einer aktiven Ansteuerung ( $\mu$ C<sub>run</sub>) eines Mikrocontrollers ( $\mu$ C) zum Einwirken auf den Mikrocontroller ( $\mu$ C) und/oder eine übergeordnete Kontrolleinheit (SG)
- 15 ausgebildet sind.
7. Vorrichtung nach dem vorhergehenden Anspruch,
- 20 d a d u r c h g e k e n n z e i c h n e t, dass die Vorrichtung zur Umsetzung eines Verfahrens nach einem oder mehreren der vorstehenden Ansprüche 1 bis 5 ausgebildet ist.
- 25 8. Vorrichtung nach einem der beiden vorhergehenden Ansprüche,
- d a d u r c h g e k e n n z e i c h n e t, dass zum Ein- oder Abschalten der Last (M) nach Vorgabe durch den Mikrocontroller ( $\mu$ C) ein Bordnetz-Steuergerät (BS) vorgesehen ist.
- 30 9. Vorrichtung nach einem der drei vorhergehenden Ansprüche,
- d a d u r c h g e k e n n z e i c h n e t, dass die gegenüber bekannten Systemen zusätzlich erforderliche Hardware im Wesentlichen in dem Mikrocontroller ( $\mu$ C) zusammengefasst ist.
- 35

10. Vorrichtung nach einem der vorhergehenden Ansprüche 6 bis 9,

5     d a d u r c h   g e k e n n z e i c h n e t, dass Diagnosemittel zur Feststellung eines Fehlerzustands vorgesehen sind, der nicht durch den Mikrocontroller ( $\mu$ C) behoben werden kann, und dass diese Diagnosemittel auch über Abhilfemaßnahmen verfügen.

## Zusammenfassung

Verfahren und Vorrichtung zur Erhöhung der Betriebssicherheit  
5 einer elektrischen Komponente

Die Diagnose einer geschalteten Hochstrom- bzw. sicherheits-  
relevanten Lasten (M) wird erweitert durch eine aktive Detek-  
10 tion einer Schaltzustandsänderung der Last (M) unabhängig vom  
Zeitpunkt der aktiven Ansteuerung des Mikrocontrollers ( $\mu\text{C}$ )  
und/oder einer übergeordneten Kontrolleinheit (SG).

Die Diagnoserückführung wird vorzugsweise auf einen „wake  
15 up“-fähigen Interrupt-Eingang des Mikrocontrollers ( $\mu\text{C}$ ) ge-  
legt. Dies ermöglicht eine aktive Diagnose bei einer Zu-  
standsänderung der Last (M), auch wenn der Controller ( $\mu\text{C}$ )  
sich im Power down mode ( $\mu\text{C}_{\text{stop}}$ ) befindet.

20

(Figur 1)

1 / 2

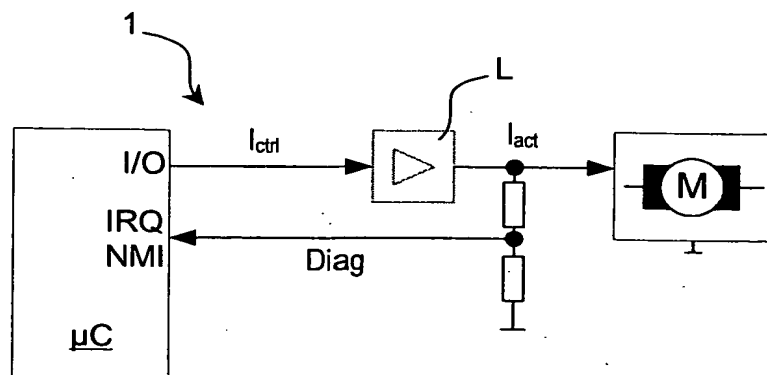


Fig. 1

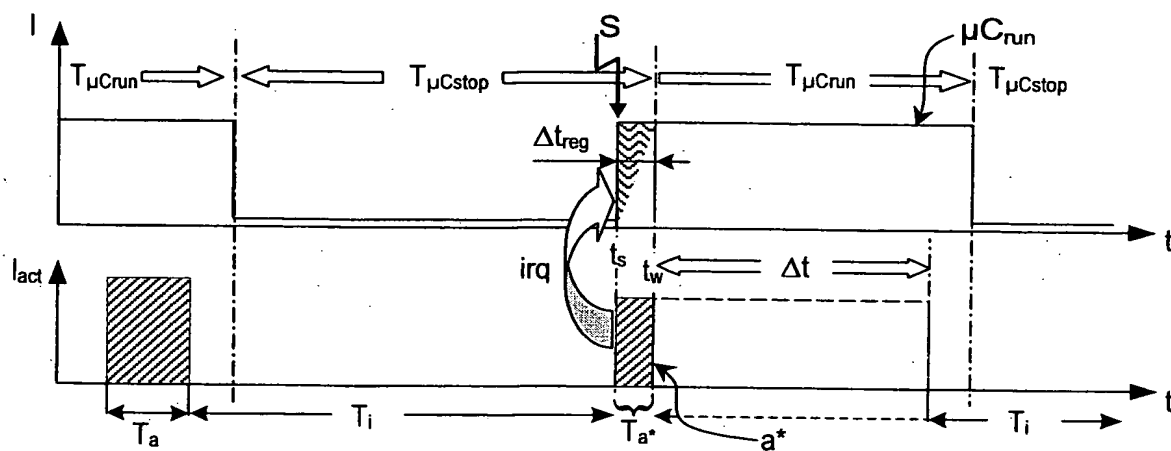


Fig. 2

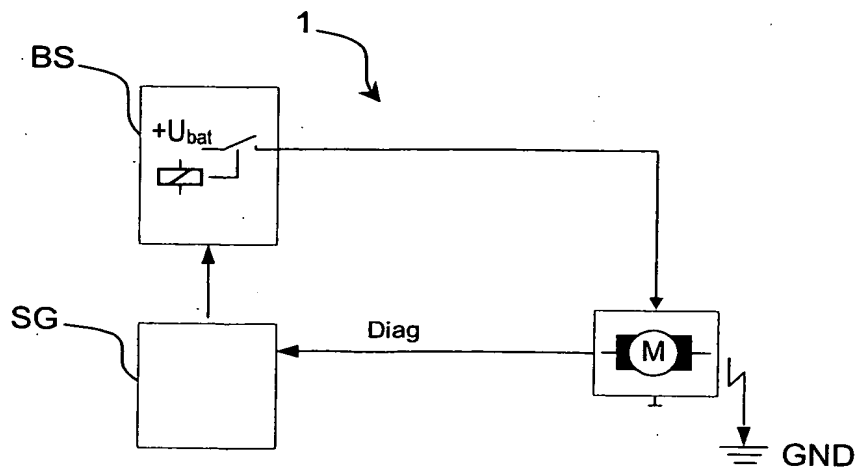


Fig. 3

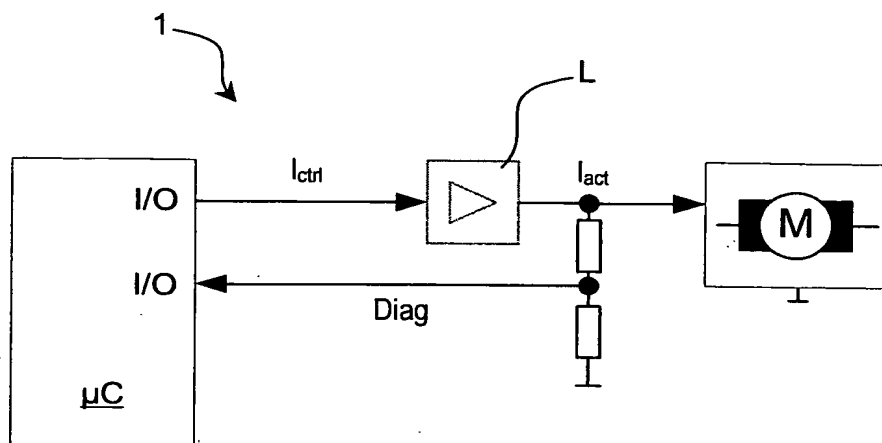


Fig. 4

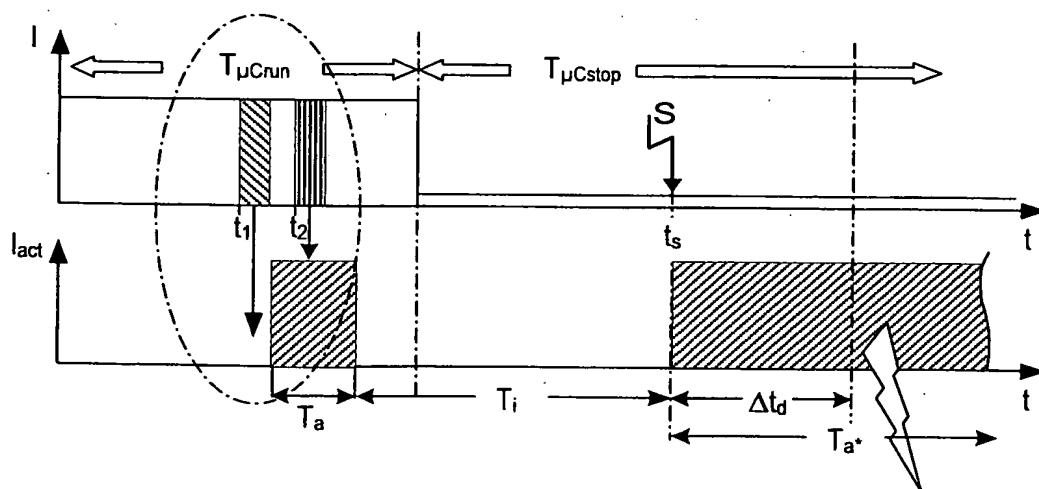


Fig. 5